



The objective is to identify :
the research gaps addressed by the
author , and to assess the scientific
contribution in this research.

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (3)

Task 7

Introduction

السلام عليكم

In this presentation, I will analyze a doctoral thesis in the field of cybersecurity, more precisely in cryptography applied to new technologies.

- ☐ The objective is to identify: the research gaps addressed by the author,
- ☐ and to evaluate the scientific contribution of this thesis.

Presentation of the thesis

The chosen thesis is:

“Post-Quantum Cryptography for Secure Cloud and IoT Systems”

Author: Michael Anderson

University: Stanford University Year: 2023

This thesis deals with a very current topic:

- securing systems against the threats of quantum computers. It proposes post-quantum cryptography solutions adapted for:
 - cloud computing
 - and IoT (Internet of Things) environments

1. Identified research gaps

The author identifies several major gaps in the literature

Gap 1: Vulnerability of classical algorithms
Current algorithms like RSA and ECC are vulnerable to quantum computing.

- Problem:
 - risk of compromise of sensitive
 - datalack of preparation of current systems

Gap 2: Low adoption of post-quantum cryptography Even though solutions exist, they are:

- poorly implemented
- poorly tested on a large scale
- There is a gap between theory and practice.

Gap 3: Constraints of IoT Environments IoT systems have:

- few resources (CPU, memory)
- energy constraints
- Post-quantum algorithms are often too heavy.

Gap 4: Lack of realistic experimental evaluation

Existing studies:

- use limited simulations
- lack real-world scenarios

2. Methodology and connection with the results

In accordance with the professor's recommendation, it is essential to link the methodology to the results.

Methodology used

The author adopts an experimental and comparative approach:

- 1) Selection of post-quantum algorithms (lattice-based, hash-based)
- 2) Implementation in simulated IoT and cloud environments

Performance

- 3) Testing
- 4) Statistical analysis (ANOVA, multi-model comparison)

Methodology link → results

Thanks to this methodology:

- ❑ algorithms are compared in a rigorous way
- ❑ performances are measured objectively

→ Results:

- ❑ improvement in security against quantum attacks
- ❑ performance varies depending on the environments
- ❑ some algorithms are suitable for IoT

Critical analysis

✓ Strength:

The comparative methodology strengthens the validity of the results

✗ Limitation:

The tests are still mostly in a simulated environment

3. Scientific contribution

This thesis makes important contributions.

❑ Contribution 1:

Adaptation of post-quantum cryptography solutions adapted to real-world environments taking into account IoT constraints

❑ Contribution 2:

Comparative evaluation rigorous comparison of algorithms identification of the most efficient ones

❑ Contribution 3:

Improvement of security protection against future quantum attacks anticipation of emerging threats

❑ Contribution 4:

Advancement of the field The thesis contributes to the development of cybersecurity in a futuristic context related to new technologies.

4. Limits of the contribution

Despite its contributions, some limitations exist:

- ❖ algorithm complexity
- ❖ high computational cost
- ❖ lack of validation in real-world conditions

5. Recommendations

To improve this research:

- 1) Test solutions in real environments
- 2) Optimize algorithms for IoT
- 3) Develop hybrid solutions (classical + post-quantum)
- 4) Encourage industrial adoption

In conclusion,

This thesis identifies significant gaps in current cryptography, including:

- ❑ the vulnerability to quantum computers
- ❑ the implementation limits in IoT systems

It makes a significant contribution by proposing post-quantum solutions adapted to new technologies.

However, real-world validations remain necessary to ensure their applicability.

Thank you for your attention.

- 1) National Institute of Standards and Technology (2022) Post-Quantum Cryptography Standardization Project
- 2) Bernstein, D. J., et al. (2017) Post-Quantum Cryptography
- 3) Alkim, E., et al. (2016)
NewHope: A Lattice-Based Key Exchange
- 1) Chen, L., et al. (2016) Report on Post-Quantum Cryptography



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

